Китайский опыт борьбы с преступлениями в сфере информационных технологий

Елена Александровна АНТОНЯН,
заведующий кафедрой криминологии и уголовно-исполнительного права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор
eaantonyan@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Аннотация. *Статья посвящена комплексному анализу системы противодействия киберпреступности в Китайской Народной Республике в условиях активного развития цифровых технологий и роста преступлений в информационном пространстве. Представлено развитие законодательства КНР в сфере кибербезопасности, включая основные нормативные акты — Закон о кибербезопасности (2017 г.), Закон о безопасности данных (2021 г.) и Закон о защите личной информации (2021 г.), а также Закон против телекоммуникационного и интернет-мошенничества (2022 г.). Рассматриваются меры усиления уголовной ответственности за IT-преступления, формирование новых составов преступлений и практика их применения. Особое внимание уделено институциональной структуре — роли правоохранительных органов и сотрудничеству с крупными технологическими компаниями. Проанализированы результаты реализации целевых кампаний, направленных на выявление и пресечение преступных схем, в том числе с использованием искусственного интеллекта, систем мониторинга интернет-трафика, технологий блокчейна и алгоритмов анализа больших данных. Подчеркивается международное изменение политики КНР в области кибербезопасности — участие в операциях Интерпола, двустороннее и многостороннее сотрудничество, продвижение концепции цифрового суверенитета. Делается вывод о высокой степени интеграции технологических, правовых и организационных механизмов в борьбе с киберпреступностью в Китае, что позволяет эффективно реагировать на современные угрозы в глобальном цифровом пространстве.*

Ключевые слова: *цифровизация, противодействие киберпреступности, Китай, мошенничество, искусственный интеллект, превентивные меры, правоохранительные органы, финансовые схемы*

DOI: 10.17803/2311-5998.2025.129.5.148-158

Elena A. ANTONYAN,
Head of the Department of Criminology
and Criminal-Executive Law
of the Kutafin Moscow State Law University (MSAL),
Dr. Sci. (Law), Professor
eaantonyan@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

China's Experience in Combating IT Crimes

Abstract. *The article is devoted to a comprehensive analysis of the system of counteracting cybercrime in the People's Republic of China (hereinafter referred to as the PRC) in the context of the active development of digital technologies and the growth of crimes in the information space. The development of the PRC legislation in the field of cybersecurity is presented, including the main regulations — the Cybersecurity Law (2017), the Data Security Law (2021) and the Personal Information Protection Law (2021), as well as the Telecommunication and Internet Fraud Prevention Law (2022). Measures to strengthen criminal liability for IT crimes, the formation of new crimes and the practice of their application are considered. Particular attention is paid to the institutional structure — the role of law enforcement agencies and cooperation with large technology companies. The results of the implementation of targeted campaigns aimed at identifying and suppressing criminal schemes, including the use of artificial intelligence, Internet traffic monitoring systems, blockchain technologies and big data analysis algorithms are analyzed. The international change of China's cybersecurity policy is emphasized — participation in Interpol operations, bilateral and multilateral cooperation, promotion of the concept of digital sovereignty. A conclusion is made about the high degree of integration of technological, legal and organizational mechanisms in the fight against cybercrime in China, which allows for an effective response to modern threats in the global digital space.*

Keywords: *digitalization, counteraction to cybercrime, China, fraud, artificial intelligence, preventive measures, law enforcement agencies, financial schemes*

В условиях стремительной цифровизации Китай, его экономика и общество, столкнулись с ростом преступлений в сфере информационных технологий. За последние пять лет в Китае последовательно наблюдается тенденция усиления мер противодействия киберпреступности: сформирована всеобъемлющая нормативно-правовая база; модернизирована работа правоохранительных органов; используются новейшие технологии — от искусственного интеллекта до сетевого мониторинга. Такие меры принесли конкретные результаты. Например,

только в 2021 г. правоохранительные органы Китая раскрыли около 400 тыс. преступлений в телекоммуникационной сфере и интернет-мошенничеств[1].

Основным законом в Китае стал Закон КНР о кибербезопасности 2017 г., установивший требования по защите сетей, хранению данных внутри страны и ответственности провайдеров. В 2021 г. были приняты сразу два важных акта: Закон о безопасности данных и Закон о защите личной информации, которые усилили ответственность компаний за утечки данных и обработку персональных сведений[2]. Эти законы обязали организации классифицировать данные по уровню важности для национальной безопасности и внедрять меры по их защите, а также ввели правила обработки персональных данных граждан, во многом аналогичные международным (с учетом практики ЕС и АСЕАН)[3].

Одновременно обновлялось китайское уголовное законодательство в части ужесточения наказания за киберпреступления. Появились специальные составы, такие как «за злоупотребление личной информацией» (незаконный сбор и сбыт персональных данных) и за «помощь в преступной деятельности в информационных сетях» (охватывает создание и распространение вредоносных программ, хакерских инструментов и пособничество онлайн-мошенникам). По данным Верховной народной прокуратуры КНР, именно преступления, связанные с использованием информационных сетей, в 2021 г. вышли на третье место по числу преступлений в стране.

Рост киберпреступности обусловил принятие новых законов, специально направленных на борьбу с наиболее распространенными ее видами. Так, нововведением стал Закон КНР против телекоммуникационного и интернет-мошенничества, принятый Постоянным комитетом Всекитайского собрания народных представителей 02.09.2022. По сути, этот Закон дополнил уголовные нормы административными санкциями за мелкие мошенничества в онлайне и детализировал меры превентивного характера. Он возложил на телекоммуникационные и финансовые структуры строгие обязанности по предотвращению мошенничества.

В частности, операторы связи и интернет-провайдеры обязаны обеспечить идентификацию пользователей (настоящее имя) при предоставлении услуг (включая мобильную связь, хостинг, обмен сообщениями, онлайн-платежи, игры и т.д.). Провайдеры должны отслеживать подозрительную активность, выявлять сомнительные аккаунты и трафик, связанный с мошенничествами, и при обнаружении требовать повторной верификации личности пользователя либо блокировать услуги. Банки и платежные системы должны мониторить необычные счета и транзакции, собирать данные об устройствах и местоположении при возникновении подозрений, а также мгновенно передавать информацию правоохранительным органам.

Тем самым устанавливается режим «должной осмотрительности» для компаний в предотвращении мошеннических действий в онлайне. В 2021 г. в стране

---

[1] URL: https://ири.рф/news/razvitie-zakonodatelstva-knr-v-oblasti-tsifrovoy ekonomiki/?ysclid=lu61e572xo553621939 (дата обращения: 30.03.2025).

[2] URL: https://www.recordedfuture.com/research/restrictive-laws-push-chinese-cybercrime-toward-novel-monetization-techniques (дата обращения: 30.03.2025).

[3] URL: https://ири.рф/news/razvitie-zakonodatelstva-knr-v-oblasti-tsifrovoy-ekonomiki/?ysclid=lu61e572xo553621939 (дата обращения: 30.03.2025).

были запрещены операции с криптовалютой (торговля, майнинг, реклама) и ужесточено регулирование в сфере отмывания средств. Все эти меры связаны с тем, что злоумышленники активно использовали криптовалюты для перевода полученных незаконным путем доходов за рубеж. Правительство КНР считает, что такие меры должны рассматриваться не как ограничение свободы, а только как необходимый шаг для защиты граждан и экономики страны от растущих киберугроз[4].

В Китае за борьбу с киберпреступностью отвечает много органов, координируемых Министерством общественной безопасности (МОВ). В его структуре создано специализированное Бюро сетевой безопасности, на которое возложена задача защиты информационных сетей и расследования преступлений в ней[5]. Аналогичные подразделения действуют в управлениях общественной безопасности провинций и городов. Кроме того, регулирование Интернета осуществляет Администрация киберпространства Китая (CAC) — орган, ответственный за цензуру и надзор за онлайн-контентом, тесно взаимодействующий с правоохранительными структурами. На каждом официально зарегистрированном веб-сайте в Китае указывается номер местного управления интернет-безопасности полиции (Public Security Bureau), ответственного за его мониторинг.

Таким образом, выстроена многоуровневая система «киберпатруля»: от центрального бюро МОВ до специальных отделов в районах, которая непрерывно отслеживает и пресекает противоправную активность в сети.

В своей деятельности китайские правоохранительные органы применяют проактивный подход, заключающийся в сочетании кибераналитики с масштабными полицейскими операциями. Ежегодно проводятся целевые кампании против наиболее острых угроз. Например, с 2020 г. в стране реализуется операция «Прерывание SIM-карт», в рамках которой полиция совместно с регуляторами связи и Народным банком Китая осуществляют контроль сети, незаконно скупаемые SIM-карты и банковские счета для использования в мошеннических целях. Только в 2021 г. в ходе такого контроля было изъято огромное количество «серых» SIM-карт и устранено свыше 30 тыс. подставных банковских счетов.

Параллельно МОВ совместно с органами, отвечающими за контроль мигрантов в стране, преследует формирования (банды), вывозящие граждан Китая за рубеж для работы в мошеннических колл-центрах. И это не случайно, поскольку многие организаторы телеком-фрода переместились в страны Юго-Восточной Азии с целью скрыться от китайской юрисдикции.

В целях повышения раскрываемости киберпреступлений внедряются новые технологии и специализированные аналитические подразделения. Примером может служить создание в г. Куньшань инновационной команды «Искусственный интеллект (AI) полиции», состоящей из 35 офицеров, использующих более 220 интеллектуальных моделей на базе больших данных, которые помогают оперативно выявлять мошеннические схемы и отслеживать перемещение денежных потоков. В результате эффективность расследований резко возросла (в 2023 г.

[4] URL: https://legascom.ru/ (дата обращения: 30.03.2025).

[5] URL: https://www.uschina.org/wp-content/uploads/2016/07/Ministry-of-Public-Security-MPS.pdf (дата обращения: 30.03.2025).

было возвращено жертвам мошенников в сети более 32 млн юаней, при этом доля возмещения по сравнению с предыдущим годом выросла на 62 %).

Известно, как в 2024 г., благодаря автоматизированному анализу, правоохранительные органы Китая за 10 минут отследили перевод 980 тыс. юаней, заблокировав половину суммы, а в течение 8 часов выявили 87 связанных подозрительных счетов, что привело к задержанию 9 преступников в течение трех дней и возврату 200 тыс. юаней пострадавшему[6]. Ранее потребовалось бы несколько недель работы группы следователей, теперь внедряемый в деятельность правоохранительных органов Китая искусственный интеллект позволяет даже малоопытным сотрудникам действовать как профессионалам высокого уровня, значительно сокращая время и повышая результативность расследований.

Изменения в законодательстве позволили существенно улучшить показатели борьбы с киберпреступностью в Китае, ежегодно раскрываются сотни тысяч таких преступлений. Так, в 2023 г. Прокуратура КНР привлекла к уголовной ответственности около 300 000 человек за различные преступления в киберпространстве (на треть больше, чем за аналогичный период 2022 г.). Наибольшую долю случаев составляют[7] интернет-мошенничества (свыше 42 000 обвиняемых в 2022 г.). Значительное число уголовных дел связано с нелегальным оборотом персональных данных (более 7 000 обвиняемых в злоупотреблениях личной информацией: торговле утечками, мошенничестве с данными). Более 1 000 человек были обвинены за преступления, угрожающие сетевой безопасности (хакерские взломы, распространение вирусов), и около 1 400 человек — за нарушения авторских прав в Интернете. Эти данные демонстрируют многопрофильный характер киберпреступности и масштаб ресурсов, которые задействует Китай для противодействия ей.

В Китае применяются масштабные превентивные меры в борьбе с киберпреступностью. Так, с 2016 по 2019 г. органы МОВ закрыли более 5 000 фальшивых веб-сайтов и 20 000 аккаунтов, выдававших себя за государственные структуры и выманивавших деньги у граждан. Причем такие сайты маскировались под официальные (содержали слова China, National и т.п. в названии), распространяя дезинформацию, мошеннические схемы «вложения в государственные фонды», даже занимались вымогательством[8]. Их ликвидация прошла в рамках целевой кампании против незаконного использования названий государственных органов. Еще одним направлением стало пресечение игорной деятельности онлайн. Дело в том, что в период пандемии COVID-19 наблюдался всплеск нелегальных азартных игр в Интернете, и к концу 2020 г. правоохранительные органы Китая начали расследование около 9 000 уголовных дел, арестовав около 50 000 подозреваемых.

Одной из характерных черт китайского подхода в борьбе с киберпреступностью является активное применение передовых технологий для выявления и

---

[6] URL: https://www.chinadaily.com.cn/a/202410/23/ws6718580ca310f1265a1c9146.html (дата обращения: 30.03.2025).

[7] URL: https://ru.apa.az/asia/kitai-nakazal-za-kiberprestupleniya-280-tys-celovek-za-11-mesyacev-559481 (дата обращения: 30.03.2025).

[8] URL: https://english.www.gov.cn/statecouncil/ministries/201911/15/content_ws5dcdfd1ac6d0bcf8c4c17220.html (дата обращения: 30.03.2025).

расследования таких преступлений. Это масштабные инструменты мониторинга интернет-трафика, системы цензурной фильтрации, в последние два года — решения на базе искусственного интеллекта.

Китайские правоохранители одними из первых начали внедрять ИИ для анализа киберпреступлений. Алгоритмы машинного обучения используются для обнаружения подозрений в сетевом трафике, распознавания мошеннических звонков и сообщений, сопоставления больших массивов данных о транзакциях. Специальные AI-команды позволяют быстро прослеживать сложные финансовые схемы, связанные с мошенничеством. Помимо этого, ИИ применяется для защиты объектов интеллектуальной собственности — автоматизированные системы отслеживают появление в сети контрафактной продукции и фишинговых сайтов, имитирующих бренды. Тестовые внедрения ИИ в ряде китайских городов позволили повысить эффективность расследования без увеличения штата сотрудников. Также ведется работа над прогнозированием киберугроз. Так, анализируя данные (например, всплески определенных схем обмана), алгоритмы могут предупредить о надвигающейся волне кибератак и вовремя применить профилактические меры.

Китай известен самой масштабной системой цензурирования Интернета, часто упоминается как проект «Золотой щит». С технической точки зрения это совокупность средств глубокого анализа пакетов (DPI), фильтрации по ключевым словам и блокировки доменов (адресов), интегрированных в узлы национальных сетей передачи данных. Первые версии системы появились еще в начале 2000-х гг., но за последние годы она значительно усложнилась. Сейчас китайские фильтры способны выявлять запрещенный контент даже при попытках обхода через VPN или прокси-серверы, мгновенно разрывая соединения. «Золотой щит» позиционируют как «общенациональный барьер, фильтрующий и контролирующий информационные потоки», призванный проверять достоверность информации и не допускать запрещенный контент[9]. Под запрещенным контентом здесь понимается не только экстремистский или порнографический материал, но и все, что противоречит законам КНР (например, сайты азартных игр, мошеннические ресурсы, хакерские форумы).

Таким образом, цензура в Китае выполняет одновременно политическую и правоохранительную функцию, делая затруднительной деятельность киберпреступников внутри страны, отсекая их коммуникационные каналы. В дополнение к техническим блокировкам китайское законодательство запретило использование несанкционированных VPN, что затрудняет злоумышленникам связь с зарубежными «теневыми» платформами: провайдеры обязаны пресекать попытки обхода цензуры.

В ответ на использование преступниками новых технологий Китай адаптирует свои подходы. Так, Народный банк Китая, в целях недопущения отмывания преступных доходов переходом на криптовалюты, внедрил системы мониторинга цепочек блокчейн-транзакций, чтобы отслеживать движения незаконных средств. В 2022 г. был принят целый комплекс мер против отмывания денег, обязывающий

[9] URL: https://legascom.ru/notes/7480-proekt-zolotoj-shchit-kak-mera-protivodejstviya-kiberprestupleniyam-v-kitajskoj-narodnoj-respublike (дата обращения: 30.03.2025).

обменники криптовалют и финтех-компании тщательнее проверять операции. В результате большинство криптобирж закрылись или ушли из Китая, а злоумышленники лишились удобного способа сокрытия прибыли.

Но есть и другой пример, когда Китай использует позитивный потенциал блокчейна: например, для хранения цифровых доказательств. С 2018 г. Верховный народный суд КНР допускает доказательства, сохраненные в блокчейне, к рассмотрению в судах, при условии обеспечения их подлинности. Правоохранительные органы экспериментируют с блокчейн-платформами для фиксирования цепочки хранения улик, с целью исключения фальсификации цифровых доказательств при расследовании.

Технологические платформы Китая также вовлечены в борьбу с киберугрозами. Крупнейшие интернет-компании (Tencent, Alibaba и др.) сотрудничают с органами МОВ, предоставляя доступ к необходимым данным при расследовании. На основании совместных приказов правоохранительных органов и регуляторов связи созданы системы раннего предупреждения: при обнаружении попытки мошеннического звонка или подозрительного сообщения возможной жертве автоматически отправляется предупреждение. Скоординированная между банками, операторами и полицией система уведомления способна определять, что звонок может исходить от мошенника, и выдать на экране телефона пользователя примерно такую надпись: «Осторожно». Кроме того, при зафиксированных случаях мошенничества полиция обязана выяснять, какие персональные данные использованы злоумышленниками, и устранять утечку в источнике. Такой подход позволяет более комплексно перекрывать возможность для повторных атак.

Важно отметить, что, усиливая технократический контроль над Интернетом, власти Китая стараются сохранять баланс между безопасностью и развитием цифровой экономики. Так называемая цифровая цензура нацелена прежде всего на криминальный и вредоносный контент. В последние годы даже наблюдается смягчение давления на IT-сектор с учетом необходимости инноваций. Например, в 2023 г. были даны сигналы о поддержке развития технологических компаний при одновременном соблюдении требований к безопасности данных. Но, несмотря на это, Интернет в Китае остается самым контролируемым в мире, что, с одной стороны, создает для киберпреступников среду, доставляющую затруднения, а с другой — заставляет их искать новые ухищрения и иногда перемещаться за пределы страны.

Понимая трансграничный характер киберугроз, Китай активно поддерживает международные усилия по их нейтрализации. КНР является членом Интерпола и регулярно пользуется его механизмами для розыска киберпреступников, скрывающихся за рубежом. Национальное центральное бюро (НЦБ) Интерпола в Пекине входит в состав Бюро международного сотрудничества МОВ. Через эту структуру китайские правоохранительные органы обмениваются разведывательной информацией о киберпреступниках с коллегами по всему миру и инициируют издание так называемых красных уведомлений на розыск преступников. Китайское НЦБ принимает активное участие в глобальных операциях Интерпола, направленных против киберпреступности и других преступлений, связанных с ней.

В частности, представители Китая регулярно задействованы в совместных рейдах, координируемых Интерполом, по пресечению сетей финансового

мошенничества, торговли данными и др. В 2021—2022 гг. проходила серия международных операций (First Light, Killer Bee и др.), направленных против телефонных мошенников, в реализацию которых китайская полиция внесла значительный вклад, особенно по линии обмена информацией о схемах и счетах, используемых преступниками. Деятельность через Интерпол помогает Китаю обнаружить преступников, скрывающихся вне его юрисдикции, и добиваться их привлечения к ответственности.

Тенденцией последних лет стала миграция части китайского криминального киберрынка за рубеж. Под давлением усиленного внутреннего контроля значительная часть криминальной активности переместилась на иностранные площадки. Опытные китайские хакеры и продавцы краденых данных все чаще действуют на англоязычных и русскоязычных теневых форумах (RaidForums, Exploit, XSS и др.), на которых они предлагают к продаже украденные банковские карты, базы данных и доступы. При этом внутри страны такие действия стали почти невозможными, поскольку постоянные операции правоохранительных и других контролирующих органов приводят к закрытию локальных нелегальных маркетплейсов и групп в мессенджерах. Преступники вынуждены шифроваться и переходить в защищенные каналы, как правило, в мессенджер Telegram, поскольку китайские форумы мониторят власти.

В последние годы Китай выстраивает тесное взаимодействие со странами Юго-Восточной Азии по вопросам борьбы с трансграничными киберпреступлениями, и прежде всего с телеком-фродом и онлайн-азартными играми. Эти виды преступлений часто организуются в соседних государствах, но нацелены на граждан КНР (их называют «заморские мошеннические фабрики»). В 2023 г. китайские власти инициировали совместные операции с Таиландом, Мьянмой, Лаосом, Камбоджей и Филиппинами, чтобы ликвидировать преступные хабы. Так, Китай вместе с партнерами провел зачистки ряда скам-комплексов в приграничных районах Мьянмы и Камбоджи, где удерживались обманом тысячи людей, которых заставляли заниматься телефонными и интернет-мошенничествами.

Китайские правоохранительные органы поделились с коллегами списками разыскиваемых лиц и методической информацией, разъясняющей: какими способами вербуются жертвы, как маскируют интернет-трафик, как переводят деньги через криптовалюты. Это позволило скоординировать рейды: например, в Таиланде при содействии Китая были отключены энергосбережение и связь у ряда подозрительных объектов вдоль границы с Мьянмой, чтобы парализовать работу мошенников. В результате только за 2023 г. Таиланд и Филиппины закрыли несколько крупных центров онлайн-казино и мошеннических колл-центров, депортировав в Китай около 1 000 китайских граждан — предполагаемых организаторов и участников этих схем. Также были освобождены сотни вовлеченных в эту деятельность обманом работников, пострадавших от траффикинга. Такой опыт признан удачным примером сотрудничества в сфере безопасности, когда страны с разными политическими системами объединяются против общей криминальной угрозы, невзирая на все разногласия.

Китай укрепляет кибербезопасное партнерство и с другими государствами. С Российской Федерацией еще в 2015 г. было подписано межправительственное Соглашение о сотрудничестве в обеспечении международной информационной

безопасности, заложившее основы обмена информацией о киберугрозах и координации действий. В тот же 2015 г., в рамках Шанхайской организации сотрудничества (ШОС), в г. Сямэнь прошли первые совместные учения Xiamen-2015 по борьбе с кибертерроризмом в сети, в которых Китай и Россия участвовали вместе с другими членами ШОС. Эти учения отработали методики совместного выявления и пресечения террористической пропаганды и координации преступников через Интернет.

С тех пор Китай регулярно выступает за усиление роли ШОС и БРИКС в вопросах обеспечения кибербезопасности. На саммитах обсуждаются идеи о создании кодекса поведения в киберпространстве и рабочих групп по противодействию киберпреступности. В 2021 г. Китай и Россия опубликовали совместное заявление о сотрудничестве в сфере международной информационной безопасности, подтвердив тем самым намерение противостоять попыткам использования ИКТ в преступных и военных целях. Помимо этого, китайские компании, обеспечивающие кибербезопасность, сотрудничают с зарубежными структурами: например, российская «Лаборатория Касперского» и китайская GETS Cyber Security заключили соглашение об обмене опытом и технологиями для борьбы с киберугрозами.

Взаимодействие с западными странами осложнено геополитическими разногласиями, Китай избирательно участвует в диалоге по вопросам борьбы с киберпреступностью. В частности, КНР поддерживает инициативы ООН: активно участвует в проекте Конвенции ООН против киберпреступности (запущен в 2019 г. при ведущей роли России) и выступает за суверенное право государств регулировать Интернет внутри своих границ.

Также Китай присоединился к ряду двухсторонних соглашений об обмене данными по киберугрозам. Например, до 2020 г. действовал механизм китайско-американских консультаций по кибербезопасности (создан в 2015 г.), позволивший на время снизить активность хакерских атак на коммерческие компании. Кроме того, китайская полиция сотрудничает с крупными транснациональными IT-корпорациями в расследовании конкретных дел. Так, в 2020 г. при поддержке Microsoft и международных экспертов китайские правоохранительные органы раскрыли одну из ботнет-сетей, использовавших сервера в разных странах для атак на китайские учреждения.

Таким образом, Китай постепенно интегрируется в глобальную систему противодействия киберпреступности, продвигая при этом собственное ви́дение «цифрового суверенитета».

За пятилетний период 2018—2023 гг. Китай достиг значительных результатов в пресечении киберпреступлений. Если в 2018—2019 гг. основной упор делался на борьбу с утечками данных и взломами (после ряда скандальных инцидентов с продажей баз персональных данных), то к 2020—2021 гг. приоритет сместился к массовым мошенничествам. В последние годы в Китае явно прослеживается консолидация криминальной активности в онлайн-среде. Многие традиционные преступления уходят в киберпространство. Такие преступные деяния, как азартные игры, мошенничество, финансовые пирамиды, все чаще осуществляются через интернет-технологии.

Одновременно появляются и совершенно новые киберпреступления, связанные с инновационными технологиями. В 2023 г. китайские правоохранители

зафиксировали первые случаи мошенничества, использующего элементы метавселенной и блокчейн-платформ: злоумышленники продавали несуществующие «виртуальные земли» и NFT-активы, оформляя их как инвестиционные проекты. Отмечается рост преступлений с применением технологии Deepfake и искусственного интеллекта. Известны многочисленные попытки выдавать себя за знакомых через сгенерированные видео или голос с целью выманивания денег. В Китае на эти вызовы реагируют прежде всего экспертные подразделения, которые, например, разработали в 2023 г. стандарты для обнаружения поддельных цифровых лиц и представили первый в стране стандарт Deepfake в финансовой сфере.

Одним из самых резонансных киберпреступлений последних лет в Китае явилась утечка в 2022 г. данных полиции Шанхая, когда хакер под псевдонимом ChinaDan выставил на продажу базу данных объемом 23 терабайта, содержащую персональные данные 1 млрд граждан Китая, включая имена, адреса, телефоны, биометрические данные. Такая утечка ведомственной базы является одним из крупнейших в мире взломов IT-системы. Этот факт ускорил принятие дополнительных мер по защите государственных информационных систем и, скорее всего, стал одной из причин огромного штрафа компании Didi, которую обвинили в недостаточной защите данных.

Другим примером, способствовавшим усилению мер безопасности в Китае, явилась многолетняя борьба с хакерской группировкой Dark Hotel, которая занималась кибершпионажем против китайских высокопоставленных лиц через заражение Wi-Fi в отелях. В 2019—2020 гг. китайские спецслужбы выявили и нейтрализовали деятельность данной группы на своей территории, что было весьма необычно, так как ранее операции Dark Hotel фиксировались в основном за рубежом. Сто́ит также отметить серию уголовных дел против хакеров внутри страны. Так, в 2018 г. правоохранительные органы Китая арестовали группу программистов, развивавших ботнет WireLoader, с помощью которого похищались учетные записи и деньги у китайских пользователей. В 2020 г. в г. Сиань были задержаны несколько человек, продававших в даркнете данные клиентов крупных отелей с информацией о 130 млн гостей.

Китай действительно преследует киберпреступников и привлекает их к ответственности по всей строгости уголовного закона, особенно если их действия направлены против внутренних интересов государства.

В области международных угроз Китай все чаще выступает не только как обвиняемый (страны Западной Европы часто заявляют о китайских арт-группах), но и как жертва кибератак. Китайские инфраструктуры регулярно подвергаются атакам извне: атакуются правительственные сайты, базы данных компаний, организаций и учреждений (в 2013 г. произошла DDoS-атака на сайт газеты «Жэньминь жибао», а ранее, в 2010 г., в результате хакерской операции была нарушена работа китайской поисковой системы Baidu на несколько часов). Китай реагирует на такие эпизоды, во-первых, усилением международного сотрудничества, требуя уважать цифровой суверенитет, во-вторых, повышением собственной киберустойчивости (создаются резервные инфраструктуры, совершенствуются национальные шифровальные стандарты).

Опыт Китая в противодействии IT-преступлениям за последние годы демонстрирует целостный и проактивный подход государства к обеспечению

кибербезопасности. За короткий срок была создана законодательная база — от Закона о кибербезопасности до специальных нормативных актов против онлайн-мошенничества, что обеспечило прозрачность в цифровой среде и дало правоохранительным структурам обоснованные дополнительные полномочия. Правоохранительные органы, опираясь на новые законы, развернули беспрецедентные по масштабу кампании по выявлению и пресечению киберпреступлений, используя как традиционные методы работы, так и современные технологии (ИИ, большие данные, автоматический мониторинг). При этом важной составляющей стало привлечение частного сектора (компании связи, интернет-платформы и банков), которые юридически обязаны помогать в предотвращении и расследовании преступлений, связанных с их сервисами.

Именно эффективные системные меры, сочетающие превентивное регулирование, четкое правоприменение и международное сотрудничество, позволяют достичь эффективности в борьбе с киберпреступностью в Китае.

Безусловно, китайский подход имеет свою специфику — значительная роль отводится контролю над информационным пространством и государственному надзору, что может быть неприменимо в странах с другими ценностными моделями. В то же время ряд элементов опыта Китая представляет интерес и для других стран: в частности, законодательное закрепление обязанностей интернет-сервисов по противодействию преступлениям; создание межведомственных систем раннего предупреждения граждан о киберугрозах; интеграция технологий ИИ в работу правоохранительных органов.

БИБЛИОГРАФИЯ

1. *Ван Г.* Уголовно-правовое регулирование противодействия киберпреступности в Китае: состояние, тенденции, недостатки // Вестник Санкт-Петербургского университета. — Право. — 2022. — Т. 13. — № 3. — С. 661—677.
2. *Се Ч.* Противодействие цифровой преступности в сфере торговли людьми в государстве АСЕАН: опыт Китая // Вестник Поволжского института права и управления. — 2025. — Т. 25. — № 1. — С. 5—13.
3. *Сюй Кай*. Законодательство о борьбе с организованной преступностью в КНР: недостатки и совершенствование // Право и государство: теория и практика. — 2010. — № 1 (61). — С. 138—142.